ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ В.Ф. УТКИНА»

Факультет вычислительной техники

Кафедра «Информационная безопасность»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

по дисциплине

Б1.О.35 «Защита в операционных системах

Специальность: 10.05.01 Компьютерная безопасность

Специализация: № 5 Разработка систем защиты информации компьютерных систем объектов информатизации" (по отрасли или в сфере профессиональной деятельности)

Квалификация выпускника: - специалист по защите информации

Форма обучения - очная

Срок обучения — 5,5 лет

Рязань 2021 г.

1 ОБЩИЕ ПОЛОЖЕНИЯ

Оценочные материалы – это совокупность учебно-методических материалов (практических заданий, описаний форм и процедур проверки), предназначенных для оценки качества освоения обучающимися данной дисциплины как части основной образовательной программы (ОПОП).

Цель – оценить соответствие знаний, умений и уровня приобретенных компетенций обучающихся целям и требованиям ОПОП в ходе проведения промежуточной аттестации.

Основная задача – обеспечить оценку уровня сформированности общекультурных и профессиональных компетенций и индикаторов их достижения, приобретаемых обучающимся в соответствии с требованиями ОПОП.

Контроль знаний обучающихся проводится в форме текущего контроля и промежуточной аттестации.

Текущий контроль успеваемости и промежуточная аттестация проводятся с целью определения степени усвоения учебного материала, своевременного выявления и устранения недостатков в подготовке обучающихся, организации работы обучающихся в ходе учебных занятий и оказания им индивидуальной помощи.

К контролю текущей успеваемости относятся проверка знаний, умений и навыков обучающихся на практических занятиях по результатам выполнения и защиты обучающимися индивидуальных заданий, по результатам выполнения контрольных работ и тестов, по результатам проверки качества конспектов лекций и иных материалов.

В качестве оценочных средств на протяжении семестра используется устные и письменные ответы студентов на индивидуальные вопросы, письменное тестирование по теоретическим разделам курса. Дополнительным средством оценки знаний и умений студентов является отчет о выполнении практических заданий и его защита.

По итогам курса обучающиеся сдают зачет и экзамен. Форма проведения – устный ответ с письменным подкреплением по утвержденным билетам, сформулированным с учетом содержания дисциплины. В билет для зачета включается два теоретических вопроса и задача. В процессе подготовки к устному ответу студент должен составить в письменном виде план ответа.

ПАСПОРТ ОЦЕНОЧНЫХ МАТЕРИАЛОВ ПО ДИСЦИПЛИНЕ

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или её части)	Вид, метод, форма оценочного мероприятия
1	2	3	4
1.	Общие вопросы безопасности ОС	ОПК-9 (ОПК-9.1, ОПК-9.2), ОПК-12 (ОПК-12.2, ОПК-12.3)	Зачет, Экзамен
2.	2. Защита в ОС Windows	ОПК-9 (ОПК-9.1, ОПК-9.2), ОПК-12 (ОПК-12.2, ОПК-12.3)	Зачет, Экзамен
3.	3. Защита в ОС Unix (Linux)	ОПК-9 (ОПК-9.1, ОПК-9.2), ОПК-12 (ОПК-12.2, ОПК-12.3)	Зачет, Экзамен
4.	4. Безопасность мобильных ОС	ОПК-9 (ОПК-9.1, ОПК-9.2), ОПК-12 (ОПК-12.2, ОПК-12.3)	Зачет, Экзамен

2 ПЕРЕЧЕНЬ КОМПЕТЕНЦИЙ С УКАЗАНИЕМ ЭТАПОВ ИХ ФОРМИРОВАНИЯ

При освоении дисциплины формируются следующие компетенции: ОПК-9 (индикаторы ОПК-9.1, ОПК-9.2) и ОПК-12 (индикаторы ОПК-12.2, ОПК-12.3).

Указанные компетенции формируются в соответствии со следующими этапами:

– формирование и развитие теоретических знаний, предусмотренных указанными компетенциями (лекционные занятия, самостоятельная работа студентов);

– приобретение и развитие практических умений предусмотренных компетенциями (практические занятия, самостоятельная работа студентов);

– закрепление теоретических знаний, умений и практических навыков, предусмотренных компетенциями, в ходе решения конкретных задач на занятиях, выполнения индивидуальных заданий на практических занятиях и их защиты, а так же в процессе сдачи зачета и экзамена.

3 ПОКАЗАТЕЛИ И КРИТЕРИи ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ (РЕЗУЛЬТАТОВ) НА РАЗЛИЧНЫХ ЭТАПАХ ИХ ФОРМИРОВАНИЯ, ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

Сформированность каждой компетенции (или ее части) в рамках освоения данной дисциплины оценивается по трехуровневой шкале:

1) пороговый уровень является обязательным для всех обучающихся по завершении освоения дисциплины;

2) продвинутый уровень характеризуется превышением минимальных характеристик сформированности компетенций по завершении освоения дисциплины;

3) эталонный уровень характеризуется максимально возможной выраженностью компетенций и является важным качественным ориентиром для самосовершенствования.

Принимается во внимание наличие и степень сформированности у обучающихся знаний, умений и обладание навыками, которые должны были формироваться в процессе изучения дисциплины.

Уровень освоения компетенций, формируемых дисциплиной:

Описание критериев и шкалы оценивания тестирования:

Шкала оценивания	Критерий
3 балла (эталонный уровень)	уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 85 до 100%
2 балла (продвинутый уровень)	уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 70 до 84%
1 балл (пороговый уровень)	уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 50 до 69%
0 баллов	уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 0 до 49%

Описание критериев и шкалы оценивания теоретического вопроса:

Шкала оценивания	Критерий
3 балла (эталонный уровень)	выставляется студенту, который дал полный ответ на вопрос, показал глубокие систематизированные знания, смог привести примеры, ответил на дополнительные вопросы преподавателя
2 балла (продвинутый уровень)	выставляется студенту, который дал полный ответ на вопрос, но на некоторые дополнительные вопросы преподавателя ответил только с помощью наводящих вопросов
1 балл (пороговый уровень)	выставляется студенту, который дал неполный ответ на вопрос в билете и смог ответить на дополнительные вопросы только с помощью преподавателя
0 баллов	выставляется студенту, который не смог ответить на вопрос

На промежуточную аттестацию (зачет, экзамен) выносится тест и два теоретических вопроса. Максимально обучающийся может набрать 6 баллов. Итоговый суммарный балл студента, полученный при прохождении промежуточной аттестации, переводится в традиционную форму по системе «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно».

Оценка «отлично» выставляется студенту, который набрал в сумме 6 баллов (выполнил все задания на эталонном уровне). Обязательным условием является выполнение всех предусмотренных в течение семестра лабораторных работ.

Оценка «хорошо» выставляется студенту, который набрал в сумме от 4 до 5 баллов при условии выполнения всех заданий на уровне не ниже продвинутого. Обязательным условием является выполнение всех предусмотренных в течение семестра лабораторных работ.

Оценка «удовлетворительно» выставляется студенту, который набрал в сумме 3 балла. Обязательным условием является выполнение всех предусмотренных в течение семестра лабораторных работ.

Оценка «неудовлетворительно» выставляется студенту, который набрал в сумме менее 3 баллов или не выполнил всех предусмотренных в течение семестра лабораторных работ.

4 ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ
4.1. Промежуточная аттестация в форме зачета

Код компетенции	Результаты освоения ОПОП Содержание компетенций
ОПК-9 (ОПК-9.1, ОПК-9.2)	Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации ОПК-9.1 Формулирует и настраивает политику безопасности операционных систем ОПК-9.2 Использует защитные механизмы и средства обеспечения безопасности операционных систем для решения задач профессиональной деятельности

Типовые практические задания (тест):

Вопрос 1

Понятие "объект" связывают с семафорамми, каналами, файлами потому, что…

Ответ:

(1) (+) их поддержка в системе связана с инкапсуляцией данных

(2) с точки зрения системы безопасности они подлежат защите от субъектов

Вопрос 2

Управление ролевым доступом предполагает…

Ответ:

(1) наличие системы управления дискреционным доступом, поскольку пользователи порождают процессы и потоки, то есть субъекты

(2) (+) приписывание пользователей к группам для упрощения администрирования

(3) (+) наличие в системе привилегированного пользователя – администратора системы

Вопрос 3

Система контроля доступа, реализованная в ОС Windows…

Ответ:

(1) позволяет формально обосновать безопасность прикладных информационных систем в большинстве случаев, представляющих практический интерес

(2) (+) полезна для декомпозиции и анализа прикладных систем, но в большинстве случаев их безопасность необходимо обосновывать путем активного исследования.

Вопрос 4

В рамках системы защиты ОС Windows каждый поток снабжается…

Ответ:

(1) (+) маркером доступа

(2) дескриптором защиты

(3) (+) идентификатором безопасности пользователя, создавшего данный поток

Вопрос 5

Дескриптор защиты в системе безопасности ОС Windows является принадлежностью…

Ответ:

(1) (+) объекта

(2) субъекта

(3) пользователя

Вопрос 6

Маркер доступа является принадлежностью…

Ответ:

(1) (+) потока

(2) (+) процесса

(3) объекта

(4) пользователя, который с помощью маркера осуществляет вход в систему

Вопрос 7

В состав учетной записи пользователя входит…

Ответ:

(1) маркер доступа

(2) дескриптор защиты

(3) (+) идентификатор безопасности SID

(4) (+) перечень привилегий пользователя в отношении системы

Вопрос 8

Учетная запись пользователя может быть создана…

Ответ:

(1) программой Winlogon в момент входа пользователя в систему

(2) (+) системным администратором при помощи административной консоли

(3) (+) при помощи функции NetUserAdd

Вопрос 9

Для удаления учетной записи можно использовать…

Ответ:

(1) (+) административную консоль управления

(2) (+) функцию NetUserDel

(3) утилиту WhoAmi.exe

Вопрос 10

Генерация идентификатора безопасности пользователя SID осуществляется…

Ответ:

(1) в момент регистрации в системе

(2) (+) при создании учетной записи

(3) (+) в результате применения функции NetUserAdd

Вопрос 11

Идентификатор безопасности SID является…

Ответ:

(1) уникальным параметром пользователя и будет одним и тем же при каждом создании учетной записи

(2) (+) параметром учетной записи, причем при каждом создании учетной записи генерируется новая версия идентификатора

Типовые теоретические вопросы:

1. Угрозы безопасности ОС: классификация угроз безопасности, типичные атаки на ОС.
2. Подходы к построению защищенных ОС.
3. Административные меры защиты. Адекватная политика безопасности.
4. Стандарты защищенности ОС.
5. Примеры защищенных ОС.
6. Типовая архитектура подсистемы защиты операционной системы.
7. Основные функции подсистемы защиты операционной системы:

Разграничение доступа к объектам операционной системы: правила разграничения доступа, разрешительная система доступа.

Идентификация, аутентификация и авторизация субъектов доступа.

Аудит: цели аудита, требования к аудиту, политика аудита.

Межсетевое экранирование.

Код компетенции	Результаты освоения ОПОП Содержание компетенций
ОПК-12 (ОПК-12.2, ОПК-12.3)	Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения ОПК-12.2 Выполняет установку, обслуживание и восстановление работоспособности компонентов общего и специального программного обеспечения ОПК-12.3 Оценивает характеристики встроенных средств защиты информации операционных систем и прикладных программ, использует и настраивает их

Типовые практические задания (тест):

Вопрос 1

Идентификатор безопасности SID…

Ответ:

(1) (+) создается в бинарной форме и может быть переведен в текстовую для визуального контроля

(2) (+) может быть введен в систему в текстовом виде и уже затем трансформирован в бинарную форму

Вопрос 2

Функция LookUpAccountName позволяет получить…

Ответ:

(1) (+) идентификатор безопасности SID по имени учетной записи

(2) имя учетной записи по идентификатору безопасности SID

Вопрос 3

Создание дескриптора защиты файла осуществляется в момент…

Ответ:

(1) открытия файла для записи

(2) (+) создания файла

Вопрос 4

Список прав доступа к файлу может содержать список…

Ответ:

(1) (+) пользователей, которым разрешено осуществлять операции с файлом

(2) (+) пользователей, которым запрещено осуществлять операции с файлом

(3) (+) операций, подлежащих аудиту

Вопрос 5

Стандартные (по умолчанию) атрибуты защиты объекта должны быть сформированы…

Ответ:

(1) непосредственно в его дескрипторе защиты

(2) (+) в маркере доступа субъекта, создающего данный объект

Вопрос 6

Список прав доступа может храниться в составе…

Ответ:

(1) (+) дескриптора защиты объекта

(2) (+) маркера доступа субъекта

Вопрос 7

При формировании входящего в состав дескриптора защиты списка прав доступа…

Ответ:

(1) (+) рекомендуется размещать запрещающие записи перед разрешающими

(2) рекомендуется размещать разрешающие записи перед запрещающими

(3) порядок расположения записей несущественен

Вопрос 8

Может ли субъект иметь дескриптор защиты?

Ответ:

(1) (+) да, поскольку субъект является частным случаем объекта

(2) нет, поскольку дескриптор защиты — это атрибут объекта

Вопрос 9

Матрица доступа описывает состояние прав доступа при…

Ответ:

(1) (+) дискреционном управлении доступом

(2) мандатном управлении доступом

(3) ролевом управлении доступом

Вопрос 10

Каналы утечки в системах с дискреционным доступом…

Ответ:

(1) (+) легко организовать

(2) существовать не могут

Вопрос 11

В некоторый момент времени t анализ системы дискреционного доступа показал, что состояние системы безопасно. Это означает, что…

Ответ:

(1) состояние системы останется безопасным и в дальнейшем

(2) (+) для того чтобы состояние системы оставалось безопасным, нужно запретить некоторые операции

(3) гарантировать, что состояние системы останется безопасным, нельзя

Вопрос 12

Чтобы сведения о попытке пользователя получить доступ к файлу попали в протокол аудита, необходимо:

Ответ:

(1) (+) предварительно внести сведения об этом пользователе в дескриптор защиты файла

(2) зафиксировать имя файла в маркере доступа пользователя

(3) внести право на доступ к файлу в состав привилегий пользователя

Вопрос 12

Список прав доступа SACL необходим для решения задач…

Ответ:

(1) контроля доступа

(2) (+) аудита

(3) аутентификации пользователей

Вопрос 13

Может ли поток, которому выделена память в стандартной куче процесса, получить случайно доступ к данным того процесса, которому эта страница принадлежала ранее?

Ответ:

(1) (+) нет, не может

(2) может

(3) может только при наличии привилегии SeSecurityPrivilege

Вопрос 14

Для того чтобы не допустить повторное использование объектов, необходимо…

Ответ:

(1) организовать эксклюзивный доступ субъектов к объектам

(2) (+) проинициализировать все объекты перед выделением новому пользователю

Вопрос 15

При передаче страниц памяти регионам в адресном пространстве процесса…

Ответ:

(1) могут использоваться только обнуленные страницы

(2) (+) иногда используются необнуленные страницы

Вопрос 16

Для защиты системных файлов от пользователя с административными правами в системе…

Ответ:

(1) для этих файлов сформированы специальные списки прав доступа

(2) (+) фиксируются изменения в этих файлах, и если файл изменен, он заменяется заранее заготовленной копией

Вопрос 17

Наиболее вероятным следствием попытки удаления администратором файла с расширением .exe из каталога %systemroot%\system32 будет…

Ответ:

(1) отказ в доступе к файлу
(2) (+) восстановление файла за счет резервной копии
(3) останов системы
(4) обычное удаление файла, например, его перемещение в корзину

Вопрос 18
Системный каталог dllcache предназначен для…
Ответ:

(1) (+) хранения резервных копий системных файлов
(2) кэширования файлов для более эффективной организации ввода-вывода
(3) кэширования динамически связываемых библиотек .dll

Вопрос 19
Предположим, что в одном из потоков процесса сформирован специальный маркер доступа для доступа к объекту. Значит, после открытия объекта остальные потоки процесса…
Ответ:

(1) (+) также будут иметь доступ к этому объекту
(2) будут иметь доступ к объекту только при наличии такого же маркера доступа
(3) не будут иметь доступа к этому объекту

Вопрос 20
Потоки одного процесса…
Ответ:

(1) имеют одинаковые маркеры доступа
(2) (+) могут иметь разные маркеры доступа

Вопрос 21
Механизм перевоплощения позволяет…
Ответ:

(1) системным потокам избежать аудита
(2) (+) связать с одним из потоков процесса маркер, отличный от маркера процесса
(3) организовать вход в систему от имени другого пользователя

Типовые теоретические вопросы:

1. Компоненты подсистемы защиты. Объекты и субъекты доступа в Windows.
2. Методы доступа к объектам в Windows.
3. Права доступа к объектам в Windows.
4. Привилегии субъектов в Windows.
5. Разрешения NTFS для файлов и папок.
6. Маркер доступа (AC) пользователя.
7. Дескриптор защиты (SD) объекта: структура дескриптора защиты, списки управления досту-

пом (DACL и SACL), маска прав в ACE, флаги в ACE - их назначение, отличие от флагов в SD, использование при наследовании.

8. Идентификатор безопасности (SID) пользователя.

9. Проверка прав доступа субъекта к объекту: общий порядок проверки SRM прав доступа субъектов к объектам, два варианта (функции) проверки прав доступа субъекта к объекту, примеры проверки прав доступа при обращении субъекта к объекту.

10. Назначение атрибутов защиты (DACL) создаваемым (новым) объектам в Windows.

11. Защита от несанкционированных действий администратора.

12. Актуальные угрозы безопасности мобильных ОС.

13. Особенности защиты в ОС Android- аутентификация и технология Smart Lock,

143. Особенности защиты в ОС Android - цифровые подписи приложений,

15. Особенности защиты в ОС Android - полномочия,

16. Особенности защиты в ОС Android - шифрование данных,

17. Особенности защиты в ОС Android - доверенная среда исполнения,

18. Особенности защиты в ОС Android - доверенная загрузка,

19. Особенности защиты в ОС Android - защита от срыва стека,

20. Особенности защиты в ОС Android - технология SELinux,

21. Особенности защиты в ОС Android - технология Seccomp,

22. Особенности защиты в ОС Android - технология SafetyNet.

23. Особенности защиты в ОС iOS.

24. Особенности защиты в ОС Android - ограничения (полномочий, API, на доступ к информации и устройствам, на работу в сети, на запуск приложений, на доступ к памяти,

4.2. Промежуточная аттестация в форме экзамена

Код компетенции	Результаты освоения ОПОП Содержание компетенций
ОПК-9 (ОПК-9.1, ОПК-9.2)	Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации ОПК-9.1 Формулирует и настраивает политику безопасности операционных систем ОПК-9.2 Использует защитные механизмы и средства обеспечения безопасности операционных систем для решения задач профессиональной деятельности
ОПК-12 (ОПК-12.2, ОПК-12.3)	Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения ОПК-12.2 Выполняет установку, обслуживание и восстановление работоспособности компонентов общего и специального программного обеспечения ОПК-12.3 Оценивает характеристики встроенных средств защиты информации операционных систем и прикладных программ, использует и настраивает их

Типовые практические задания (тест):

Вопрос 1

В ОС Windows реализована система управления…

Ответ:

(1) дискретным доступом

(2) (+) дискреционным доступом

(3) (+) привилегированным доступом

Вопрос 2

В ОС Windows матрица доступа в силу ее большого размера и разреженности хранится в виде набора…

Ответ:

(1) (+) дескрипторов защиты объектов

(2) маркеров доступа процессов

Вопрос 3

В системе защиты ОС Windows процедура входа в систему Winlogon …

Ответ:

(1) функционирует в режиме ядра

(2) (+) является системным процессом пользовательского режима

Вопрос 4

В соответствии с политикой безопасности, лежащей в основе системы защиты ОС Windows …

Ответ:

(1) (+) владелец ресурса может контролировать доступ к нему

(2) доступ к ресурсу может контролировать только системный администратор

Вопрос 5

Привилегии конкретного пользователя ОС Windows…

Ответ:

(1) (+) назначаются администратором системы

(2) специфицируются стандартами, в частности "оранжевой" книгой.

Вопрос 6

Администратор системы…

Ответ:

(1) всегда обладает всеми привилегиями

(2) (+) обладает лишь некоторыми привилегиями в соответствии с минимумом привилегий

Вопрос 7

Изменить системное время может…

Ответ:

(1) только администратор системы

(2) любой пользователь

(3) (+) пользователь, обладающий соответствующей в отношении системы привилегией

Вопрос 8

Каждая привилегия в отношении системы специфицируется:

Ответ:

(1) (+) внутренним номером

(2) (+) программным именем

(3) (+) дружественным именем

Вопрос 9

Для того чтобы лишить пользовательское приложение конкретной привилегии в отношении системы, достаточно…

Ответ:

(1) перед запуском приложения удалить эту привилегию из учетной записи пользователя

(2) (+) отключить данную привилегию в маркере доступа приложения

Вопрос 10

Маркер доступа содержит…

Ответ:

(1) только привилегии, перечисленные в учетной записи пользователя

(2) (+) совокупность привилегий пользователя и групп, к которым приписан данный пользователь

Вопрос 11

Для того чтобы добавить новую привилегию в маркер доступа процесса, достаточно…

Ответ:

(1) после запуска процесса вызвать одну из функций, добавляющих привилегию, например, LsaAddAccountsRights

(2) перед стартом процесса добавить данную привилегию в учетную запись пользователя, от имени которого запускается процесс

(3) (+) перед стартом процесса добавить данную привилегию в учетную запись пользователя, от имени которого запускается процесс, и организовать для этого пользователя повторный вход в систему

(4) (+) перед стартом процесса добавить данную привилегию в учетную запись пользователя, от имени которого запускается процесс, и осуществить перезагрузку системы

Вопрос 12

Сколько привилегий обычно содержит учетная запись пользователя с административными правами в ОС Windows 2000 непосредственно после ее создания?

Ответ:

(1) (+) 0

(2) 17

Вопрос 13

Функция LsaAddAccountsRights позволяет добавить привилегию в:

Ответ:

(1) маркер доступа процесса

(2) (+) учетную запись пользователя

Вопрос 14

Функция LsaRemoveAccountRights позволяет отозвать привилегию из:

Ответ:

(1) маркера доступа процесса

(2) (+) учетной записи пользователя

(3) электронной почты администратора

Вопрос 15

Процедура аутентификации пользователя обычно инициируется…

Ответ:

(1) (+) комбинацией клавиш SAS (secure attention sequence)

(2) (+) комбинацией клавиш "ctrl+alt+del"
(3) случайной комбинацией символов, генерируемых драйвером клавиатуры

Вопрос 16
Смысл использования комбинации клавиш "ctrl+alt+del" состоит в том, что она…
Ответ:

(1) легко запоминается пользователем
(2) (+) всегда перехватывается драйвером клавиатуры, который вызывает подлинную программу аутентификации
(3) используется для аутентификации по умолчанию и легко может быть заменена на любую другую

Вопрос 17
Главное отличие штатной интерактивной процедуры аутентификации от троянского коня заключается…
Ответ:

(1) (+) в том, что она инициируется последовательностью клавиш "ctrl+alt+del", перехват которой драйвером клавиатуры отменить нельзя
(2) во внешнем виде и структуре диалогов

Вопрос 18
Применив комбинацию клавиш "ctrl+alt+del", пользователь может…
Ответ:

(1) (+) зарегистрироваться в системе
(2) (+) посмотреть список активных процессов
(3) (+) инициировать перезагрузку
(4) (+) заблокировать компьютер

Вопрос 19
Вся необходимая информация для формирования маркера доступа находится в…
Ответ:

(1) учетной записи пользователя
(2) ключах реестра
(3) (+) учетной записи пользователя и ключах реестра

Вопрос 20
Чтобы сформировать новый маркер доступа, можно…
Ответ:

(1) (+) осуществить регистрацию в системе
(2) (+) вызвать функцию `LogonUser`
(3) извлечь его из раздела `SECURITY` реестра

Вопрос 21
Система аудита заключается в…
Ответ:

(1) (+) протоколировании действий пользователей и использовании полученных протоколов для выявления вторжений

(2) проверки подлинности пользователей при помощи паролей или биометрических средств

(3) проверки прав доступа к объекту на основе списков ACL

Вопрос 22

Для правильной организации регистрации пользователя в системе целесообразно…

Ответ:

(1) **(+)** применить процедуру аутентификации для установления подлинности пользователя

(2) **(+)** применить процедуру аудита, так как данное событие относится к категории потенциально опасных

(3) проверить наличие привилегии пользователя на вход в его маркере доступа

Типовые теоретические вопросы:

1. Процессы-серверы в Windows: подходы к выполнению привилегированных действий в Windows (временное получение дополнительных полномочий (полномочий другого пользователя), обращение к услугам процесса-сервера), процесс-серверы в Windows, олицетворение пользователя.
2. Аудит и обнаружение атак в Windows: журнал аудита, политика аудита, типы регистрируемых событий, использование информации из журнала аудита для анализа (анализ попыток регистрации, анализ доступа к объектам, анализ выполняющихся задач (отслеживание процессов).
3. Анализ использования привилегий, анализ событий с учетными записями, анализ изменения политик).
4. Требования к политике аудита. Администраторы и аудиторы (разделение).
5. Внедрение вредоносных программ через реестр и планировщик заданий Windows: структура и расположение реестра, ключи автозагрузки для внедрения потенциально опасных программ (8 случаев).
6. Планировщик заданий в Windows, средства контроля автозагрузки.
7. Политики ИПС, SRP и Applocker: подходы к созданию изолированной программной среды до Windows XP, политика ограниченного использования программ (SRP). Политика Applocker и ее сравнение с SRP.
8. Механизм идентификации, аутентификации и авторизации в Windows: структура механизма идентификации и аутентификации, виды (типы) входа в систему, идентификация и аутентификация с помощью msv1_0(NTLM) - верхний, средний и нижний уровни, идентификация и аутентификация с помощью Kerberos v.5.
9. Провайдеры сетевой аутентификации, параметры идентификации и аутентификации в Windows, Credential Provider'ы (поставщики учетных данных) в ОС Windows Vista и выше.
10. Особенности защиты в серверных версиях ОС Windows.
11. Компоненты подсистемы защиты в Unix (Linux).
12. Объекты и субъекты доступа в в Unix (Linux).
13. Разграничение доступа в Unix (Linux).
14. Встроенные средства шифрования Unix (Linux).
15. Аудит и обнаружение атак в ОС Unix (Linux).
16. Идентификация, аутентификация и авторизация пользователей в ОС Unix (Linux).
17. Процессы-серверы в ОС Unix (Linux).
18. Внедрение вредоносных программ в ОС Unix (Linux).
19. Особенности защиты в серверных версиях ОС Unix (Linux).

Составил
к.т.н., доцент кафедры
«Информационная безопасность» Ю.М. Кузьмин